Abstract of the Disclosure

By providing a unit receiving the input of a set T of bit numbers that are obtained by unequally dividing all the bit numbers of input data to be given to a computing apparatus, a unit outputting a value A_T indicating an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes of which the input and output bit numbers are equivalent to the divided bit numbers, a unit determining that an appropriate linear converting unit is present when the value of A_T is positive, and a unit forming a pseudo MDS matrix as the linear converting unit, computation is executed using a unit with an excellent data diffusion performance as the linear converting unit in SPN structure, when the input number is not the same as the output number among a plurality of S boxes of the SPN structure in an F function.